Robert C. Schubert (No. 62684)
Amber L. Schubert (No. 278696)
Schubert Jonckheer & Kolbe LLP
2001 Union St Ste 200
San Francisco, CA 94122
Ph: 415.788.4220
Fx: 415.788.0161
rschubert@sjk.law
aschubert@sjk.law

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MOIRA DUFFY, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION, WELLTOK, INC., and SUTTER HEALTH, Defendants.	Case No. **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiff Moira Duffy ("Plaintiff"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against Progress Software Corporation ("PSC"), Welltok, Inc. ("Welltok"), and Sutter Health (collectively, "Defendants"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action lawsuit on behalf of all persons who entrusted Defendants with sensitive personal information that was exposed in a data breach when, on or about May 30, 2023, an unauthorized third party accessed Welltok's internal MOVEit Transfer servers, which contained individuals' sensitive personally identifying information ("PII") and personal health information ("PHI") (the "Data Breach" or the "Breach").

2. PSC is a software company that offers software products and services to corporate and governmental entities, including cloud hosting and secure file transfer services such as MOVEit.

3. Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Sutter Health. Welltok received the PII for Sutter Health's patients in connection with these services. Welltok uses PSC's MOVEit file transfer services.

4. Sutter is a large healthcare system based in Sacramento, which contracted with Welltok to provide communications to its patients and shared their PII.

5. Plaintiff's claims arise from Defendants' failure to safeguard Plaintiff's and Class members' PII. Plaintiff's and Class members' PII was compromised due to Defendants' negligent and/or careless acts and the failure to protect their PII.

6. In carrying out its services, Welltok utilizes MOVEit, the file sharing application created and operated by PSC, to securely transmit files containing sensitive patient information. On or about May 30, 2023, Welltok received a notification from PSC that an unauthorized external party had exploited a vulnerability within the MOVEit software. Welltok then initiated an inquiry and determined that the unauthorized party had gained entry to one of Welltok's

MOVEit Transfer servers on May 30, 2023. During this time, the unauthorized party acquired data containing sensitive PII held by Welltok and belonging to Sutter patients.

7. The hackers responsible for the Data Breach were subsequently identified as the Russian cyber gang, Clop.[1]

8. Plaintiff and members of the Class furnished sensitive and private PII directly or indirectly to Sutter and Welltok, including their names, dates of birth, and health insurance information. Sutter also kept and provided additional sensitive and private PII to Welltok, including provider names, treatment cost information, and treatment information and diagnoses.

9. Defendants failed to properly secure and safeguard Plaintiff's and the Class's PII that was stored within the MOVEit servers.

10. Despite purporting to act as a safe container for sensitive information, Defendants failed to take precautions designed to keep that information secure.

11. The data that Defendants exposed was highly sensitive, including names, dates of birth, health insurance information, provider names, treatment cost information, and treatment information and diagnoses.

12. The Data Breach affecting PSC's MOVEit file transfer tool impacted tens of millions of individuals in the United States, including 845,000 Sutter patients.[2]

13. The sensitive nature of the data exposed through the Data Breach, including private health insurance and health care information, substantiates that Plaintiff and Class

---

[1] Onur Demirkol, *US Government Under Siege: MOVEit Breach Exposes Critical Data to Ruthless Clop Ransomware Attack*, DATA CONOMY (June 19, 2023), available at https://dataconomy.com/2023/06/19/moveit-breach-data-clop-ransomware/ (last visited September 11, 2023).

[2] *See* Carly Page, *Millions affected by MOVEit mass-hacks as list of casualties continues to grow*, TECHCRUNCH https://techcrunch.com/2023/06/29/millions-affected-moveit-mass-hacks/ (last visited September 11, 2023).

members have suffered irreparable harm. Plaintiff and Class members have lost the ability to control their private information and are subject to an increased risk of identity theft.

14. Defendants owed and owe a duty to Plaintiff and Class members to maintain adequate security measures to safeguard the PII with which they were entrusted with. Defendants breached their duty by failing to implement and/or maintain adequate security practices.

15. Sutter and Welltok delayed acknowledging and giving notice of the Data Breach. Sutter and Welltok did not notify its customers of the Data Breach until late October 2023 at the earliest (the "Notice Letter"). *See*, *e.g.*, Plaintiff Duffy's Notice Letter, attached hereto as Exhibit A Notice Letter. Sutter and Welltok waited despite knowing that hackers accessed patients' information, and that sensitive PII and PHI was compromised.

16. As a result of Sutter and Welltok's inadequate digital security and notice process, Plaintiff's and Class members' PII and PHI was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries including financial losses caused by misuse of PII and PHI; the loss or diminished value of their PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal, medical, and financial information.

17. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendants for negligence; negligence *per se*; breach of implied contract; breach of implied covenant of good faith and fair dealing; breach of fiduciary duty; unjust enrichment; and declaratory judgment and on behalf of a California Subclass against Defendants for violation of the California Unfair Competition Law; violation of the California Consumer Records Act; violation of the California Consumer Legal Remedies Act; and violation of the California Confidentiality of Medical Information Act.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

19. This Court has personal jurisdiction over Defendants because they conduct substantial business in this jurisdiction. Further, this Court has general jurisdiction over Defendant Sutter Health because it is a California corporation and its corporate headquarters is located in this State.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Plaintiff is located in this District and provided her PII and PHI to Sutter Health in this District; defendant Welltok received Plaintiff's PII and PHI from Sutter Health in this District; and defendant PSC designed, marketed, sold, and maintained the MOVEit transfer application in this District.

21. Intradistrict Assignment: Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Francisco Division of the Northern District of California is proper because a substantial part of the events or omissions which give rise to the claim occurred in this Division or a substantial part of the property subject to the action is situated in this Division. Plaintiff is located in this Division and provided her PII and PHI to defendant Sutter in this Division. Defendants are also engaged in the extensive promotion, marketing, distribution, and sales of the products at issue in this Division.

PARTIES

22. Plaintiff Moira Duffy is a citizen of California and resides in San Francisco, California. Plaintiff Duffy received the Notice Letter dated October 31, 2023, notifying her that her information was part of the Data Breach. Plaintiff Duffy is currently a patient at the Pacific Women's OB/GYN Medical Group, which is part of Sutter California Pacific Medical Center, located at 1375 Sutter Street in San Francisco, California. She has been a Sutter Health patient since approximately October 2021.

23. Plaintiff Duffy has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft and financial and medical fraud. Plaintiff Duffy fears for her personal financial and health security and uncertainty over what PII and PHI was exposed in the Data Breach.

24. Plaintiff Duffy was required to provide her PII/PHI to Sutter in connection with obtaining healthcare or other services.

25. Based on representations made by Sutter and relied upon by Plaintiff Duffy, Plaintiff Duffy believed that Sutter had implemented and maintained reasonable security and practices to protect her PII/PHI, including ensuring third parties it contracts with and shares PII/PHI with maintain adequate data security and practices.

26. In connection with providing healthcare or other services to Plaintiff Duffy, Sutter collected, maintained, and shared Plaintiff Duffy's PII/PHI on its systems and to its vendors, including Welltok.

27. Had Plaintiff Duffy known that Defendants do not adequately protect the PII/PHI in their possession, including Sutter and Welltok by not ensuring that the third parties they

contract with maintain adequate data security systems and practices, she would not have agreed to provide her PII/PHI to Sutter.

28. Defendant Progress Software Corporation is a corporation organized under the laws of the State of Delaware with its principal place of business located in Burlington, Massachusetts.

29. Defendant Welltok, Inc. is a Delaware corporation with its principal place of business located in Providence, Rhode Island.

30. Defendant Sutter Health is a California nonoprofit corporation with its principal place of business located in Sacramento, California.

FACTUAL BACKGROUND

The Data Breach

31. On or about May 31, 2023, PSC, the creator of the MOVEit software, Progress Software, announced on its Progress Community website that it was subject to a Data Breach,[3] which compromised highly sensitive PII/PHI of those that utilize the MOVEit software including names, dates of birth, health insurance information, provider names, treatment cost information, and treatment information and diagnoses.

32. Welltok employs the MOVEit software, which is supplied by PSC. MOVEit's intended use is to safely move files as part of their routine operations. Within this process, Welltok uploads, retains, shifts, or retrieves PII/PHI owned or held by various companies on whose behalf it provides its various services. Sutter shared this data with Welltok, which managed it using the MOVEit software.

[3] MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362), Progress Community, https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last accessed September 12, 2023).

33. On or about July 26, 2023, PSC informed Welltok of a vulnerability in the MOVEit software that was exploited by an unauthorized third party.

34. Welltok reportedly performed an internal investigation into the scope of the vulnerability in MOVEit's software and the impact on its systems.[4] Welltok's investigation revealed that the third party exploited software vulnerabilities, accessed its MOVEit transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit transfer server during that time.[5]

35. On August 11, 2023, Welltok completed its investigation and confirmed the identities of individuals affected by the Data Breach.[6]

36. Individuals impacted by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

37. Plaintiff and Class members are or were Sutter patients customers who entrusted Sutter (and in turn, Welltok) with their PII/PHI.

Sutter and Welltok's Obligation and Responsibility to Protect Plaintiff and Class members' PII/PHI

38. Sutter provides healthcare to "more than 3 million Californians."[7] The company has over 51,000 employees and 22 hospitals, among other locations.[8]

39. According to its notice letter, Welltok "operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices

[4] *See* Exhibit A.
[5] *Id.*
[6] *Id.*
[7] *What is Sutter Health*, Sutter Health, https://www.sutterhealth.org/about/what-is-sutter-health (last accessed Jan. 9, 2024).
[8] *Id.*

and communications."[9]

40. Sutter maintains a privacy policy on its website that states, "Federal and state laws require Sutter Health to protect your health information …."[10] The privacy policy also states, "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[11]

41. Sutter's Patient Rights and Responsibilities also discusses privacy, stating that patients have a right to "[c]onfidential treatment of all communications and records pertaining to your care and stay in the hospital."[12]

42. Sutter shared Plaintiff's and Class members' PII/PHI with Welltok, who then shared the PII/PHI with PSC via the MOVEit software in connection with providing services to Plaintiff and Class members.[13] In doing so, Sutter failed to ensure that Welltok would adequately protect its patients' PII/PHI, and Welltok failed to ensure that PSC implemented and maintained adequate data security practices to protect Plaintiff and Class members' PII/PHI from unauthorized access, disclosure, and theft.

43. As a healthcare provider that handles patients' personal and health information, Sutter is legally required to protect PII/PHI from unauthorized disclosure.

Sutter and Welltok's Failure to Prevent, Identify, and Timely Report the Data Breach

44. Sutter and Welltok failed to take adequate measures to protect its computer systems and internal network against unauthorized access.

---

[9] Ex. A.

[10] *HIPAA and Privacy Practices*, Sutter Health, https://www.sutterhealth.org/privacy/hipaa-privacy (last accessed Jan. 9, 2024).

[11] *Id.*

[12] *Patient Rights and Responsibilities*, Sutter Health, https://www.sutterhealth.org/for-patients/patient-rights-responsibilities (last accessed Jan. 9, 2024).

[13] Ex. A

45. Sutter and Welltok also failed to properly select its information security partners that it relied upon to keep the PII/PHI it held safe and secure.

46. Sutter and Welltok were not only aware of the importance of protecting the PII/PHI that it maintains, but they also touted theircapability to do so. The PII/PHI that was exposed in the Data Breach is the type of private information that Sutter and Welltok knew or should have known would be the target of cyberattacks.

47. Despite its own knowledge and supposed expertise concerning cybersecurity, and notwithstanding the Federal Trade Commission's (FTC's) data security principles and practices,[14] Sutter and Welltok failed to disclose that its systems and security practices were inadequate to reasonably safeguard sensitive personal information.

48. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[15] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves. Despite this guidance, Sutter and Welltok delayed the notification of the Data Breach for over three months.

Defendants Failed to Comply with Regulatory Requirements and Industry Practices

49. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

---

[14] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited September 11, 2023).

[15] *Id*.

50. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain Private Information, about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

51. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[16]

52. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[18] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed;

---

[16] *See Addressing BPO Information Security: A Three-Front Approach*, Datamark, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security.

[17] *Start With Secuirty,* Fed. Trade Comm'n, at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 22, 2023).

[18] *Protecting Personal Information: A Guide for Business*, ed. Trade Comm'n, https://www.ftc.ov/ system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 22, 2023).

encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

54. The FTC also recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

55. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information and failure to segregate access to information50 may violate the FTC Act.

[19] *Start With Secuirty,* Fed. Trade Comm'n, at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 22, 2023).

57. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data (i.e., Private Information) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Furthermore, Defendants are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

59. The Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[20]

60. Pursuant to HIPAA's mandate that Defendants follow "applicable standards, implementation specifications, and requirements … with respect to electronic protected health information," 45 C.F.R. § 164.302. Defendants were required to, at minimum, to "review and

[20] Summary of the HIPAA Security Rule, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Aug. 22, 2023).

modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

61. Defendants are also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

62. Both HIPAA and HITECH obligate Defendants to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. §17902.

63. As alleged in this Complaint, Defendants have failed to comply with HIPAA and HITECH. They have failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of protected health information.

64. Additionally, cybersecurity experts have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems;

protection against any possible communication system; and training staff regarding critical points.[21] Defendants did not follow such minimum best practices.

The Current and Future Harms Caused by the Data Breach

65. Victims of data breaches are susceptible to becoming victims of identity theft.

66. Plaintiff and Class Members face a lifetime of constant surveillance of their financial, personal, and health records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damage in addition to any fraudulent use of their PII/PHI.

67. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.

68. PII/PHI is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[22]

69. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

[21] *See Addressing BPO Information Security: A Three-Front Approach*, Datamark, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security.

[22] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on- the-dark-web-how-much-it-costs.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

70. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, in that situation, victims can cancel or close payment card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, health insurance information, and health records.

71. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[24] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers or health insurance information.

72. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[25] According to a report released by the Federal Bureau of Investigation's

---

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[24] *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Aug. 22, 2023).

[25] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentialsfetch- high-prices-in-the-online-black-market.

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[26]

73. Identity thieves may use stolen data to commit health care fraud, prescription drug fraud, bank fraud, credit card fraud, employer or tax-related fraud, government documents or benefits fraud, loan or lease fraud, phone or utilities fraud, among other forms of fraud.[27]

74. Criminals can use stolen PII to extort a financial payment by "leveraging details specific to a disease or terminal illness."[28] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion. … By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[29]

75. Cybercriminals took the PII/PHI of Plaintiff and Class Members to engage in identity theft, healthcare fraud, and/or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activities resulting from the Data Breach may not come to light for years.

---

[26] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber- intrusions.pdf.

[27] FTC Consumer Sentinel Network, Compare Identity Theft Report Types, https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime, (Last visited July 9, 2023).

[28] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcaredata- perfcon ("What Happens to Stolen Healthcare Data") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[29] Id.

76. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[30]

77. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

78. Identity theft, which costs Americans billions of dollars annually, occurs when an individual's PII is used without consent to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime and hundreds, if not thousands, of dollars.

79. According to Javelin Strategy & Research, in 2018 alone, identity theft affected over 16.7 million individuals, causing a loss of over $16.8 billion.

80. Recent FTC data reveals that identify theft remains the top category of fraud reports received by the agency.[31] The FTC received over 1,100,000 reports of identity theft in 2022, and over 280,000 for the first quarter of 2023 alone.[32]

81. Identity thieves use personal information for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[33] According to Experian, one of the

---

[30] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO.

[31] FTC Consumer Sentinel Network, Federal Trade Commission, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState, (Last visited July 9, 2023).

[32] *Id*.

[33] The FTC defines identity theft as "a fraud committed or attempted using the identifying

largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[34]

82. With access to an individual's PII, criminals can do more than just empty a victim's bank account. They can also commit all manner of fraud, including (i) obtaining a driver's license or official identification card in the victim's name but with the thief's picture; (ii) using the victim's name and SSN to obtain government benefits; or (iii) filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[35]

83. Consumers place a high value not only on their personal information but also on the privacy of that data. They do so because identity theft causes "significant negative financial impact on victims" in addition to severe distress and other strong emotional and physical reactions.

---

information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[34] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-canidentity- thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Mar. 21, 2022).

[35] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Mar. 21, 2023); *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES.

84. The United States Government Accountability Office ("GAO") explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name."[36] The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

85. Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as well as a lapse between when the PII/PHI is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

86. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[39]

---

[36] *See* Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. Government Accountability Office Report to Congressional Requesters ("GAO Report") at 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf, (Last visited July 10, 2023).

[37] Id.

[38] *See* GAO Report, at p.29.

[39] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited September 11, 2023).

87. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[40] Defendants did not rapidly or timely report to Plaintiff and Class members that their PII/PHI had been stolen.

88. As a result of the Data Breach, Plaintiff and Class members' PII/PHI has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered thereby as a direct result of Defendants' Data Breach, include:

a. unauthorized use of their PII/PHI;

b. theft of their personal, financial, and helathinformation;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial and healthcare accounts;

d. damages arising from the inability to use their PII/PHI;

e. Improper disclosure of their PII/PHI;

f. loss of privacy and embarrassment;

g. trespass and damage their personal property, including PII/PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and

[40] *Id*.

identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being placed in the hands of criminals and already misused via the sale of Plaintiff and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII/PHI entrusted to Defendants.

89. In addition to a remedy for economic harm, Plaintiff and Class members maintain an interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft.

90. Defendants disregarded the rights of Plaintiff and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that Defendants did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and Class members' PII/PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to provide Plaintiff and Class members prompt notice of the Data Breach.

91. The actual and adverse effects to Plaintiff and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud, and medical fraud directly or proximately caused by Defendants' wrongful actions or inaction and the resulting Data Breach require Plaintiff and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently

obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes, and closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

92. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> **All persons in the United States whose PII/PHI was compromised in the Data Breach announced by Sutter and Welltok on October 31, 2023.**

93. Plaintiff also brings this action on behalf of the following California Subclass:

> **All persons in California whose PII/PHI was compromised in the Data Breach announced by Sutter and Welltok on October 31, 2023.**

94. Specifically excluded from the Class and Subclass are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

95. Plaintiff reserves the right to amend the Class and Subclass definitions above if further investigation and/or discovery reveals that the Class or Subclass should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

96. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

97. Numerosity (Rule 23(a)(1)): The Class and Subclass are so numerous that joinder of all Class and Subclass members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendants, Plaintiff estimates that the Class is comprised of at least hundreds of thousands of Class members. The Class and Subclass are sufficiently numerous to warrant certification.

98. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class members because they all had their PII/PHI compromised as a result of the Data Breach. Plaintiff is a member of the Class and Subclass and her claims are typical of the claims of the members of the Class and Subclass. The harm suffered by Plaintiff is similar to that suffered by all other Class and Subclass members that was caused by the same misconduct by Defendants.

99. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class and Subclass. Plaintiff has no interest antagonistic to, nor in conflict with, the Class or Subclass. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation, including data breach class actions, and who will prosecute this action vigorously.

100. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class and Subclass members is relatively small, the expense and burden of individual litigation make it impossible for individual Class and Subclass members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for their wrongdoing as asserted herein.

101. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class and Subclass members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
b. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
c. Whether Defendants' storage of Class and Subclass Member's PII/PHI was done in a negligent manner;
d. Whether Defendants had a duty to protect and safeguard Plaintiff and Class and Subclass members' PII/PHI;
e. Whether Defendants' conduct was negligent;
f. Whether Defendants' conduct violated Plaintiff and Class and Subclass members' privacy;
g. Whether Defendants took sufficient steps to secure their patients' PII/PHI;
h. Whether Defendants were unjustly enriched;
i. The nature of relief, including damages and equitable relief, to which Plaintiff and members of the Class and Subclass are entitled.

102. Information concerning Defendants' policies is available from Defendants' records.

103. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

104. The prosecution of separate actions by individual members of the Class and Subclass would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

105. Defendants have acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate final injunctive relief and/or corresponding declaratory relief with respect to the Class and Subclass as a whole.

106. Given that Defendants have not indicated any changes to their conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
On Behalf of the Nationwide Class Against All Defendants

107. Plaintiff repeats and realleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

108. Plaintiff brings this claim individually and on behalf of the Class members.

109. Defendants knowingly collected, came into possession of, and maintained Plaintiff and Class members' PII/PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

110. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class members' PII/PHI.

111. Defendants had, and continue to have, a duty to timely disclose that Plaintiff and Class members' PII/PHI within their possession was compromised and precisely the type(s) of information that were compromised.

112. Defendants owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards, applicable standards of care from statutory authority

like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected their customers' PII.

113. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their customers. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

114. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards and state and federal laws to protect confidential PII/PHI.

115. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class members' PII/PHI.

116. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII/PHI;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to adequately and timely notify impacted consumers of the Data Breach; and

e. Failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

117. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class members' PII/PHI within Defendant's possession.

118. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class members' PII/PHI.

119. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class members that the PII/PHI within Defendant's possession might have been compromised and precisely the type of information compromised.

120. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff and Class members' PII/PHI would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

121. It was foreseeable that the failure to adequately safeguard Plaintiff and Class members' PII/PHI would result in injuries to Plaintiff and Class members.

122. Defendants' breaches of duties owed to Plaintiff and Class members caused Plaintiff and Class members' PII/PHI to be compromised.

123. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

124. As a result of Defendants' failure to timely notify Plaintiff and Class members that their PII/PHI had been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

125. As a result of Defendants' negligence and breach of duties, Plaintiff and Class members are in danger of imminent harm in that their PII/PHI, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the

compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
On Behalf of the Nationwide Class Against All Defendants

126. Plaintiff realleges and incorporate by reference herein all the allegations contained above.

127. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair … practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiff and Class members' PII/PHI. Various FTC publications and orders also form the basis of Defendants' duty.

128. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff and Class members' PII/PHI and not complying with industry standards.

129. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI obtained and stored and the foreseeable consequences of a data breach.

130. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

131. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

132. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

133. As a result of Defendants' negligence, Plaintiff and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
On Behalf of the Nationwide Class Against All Defendants

134. Plaintiff repeats and realleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

135. Plaintiff and the Class provided and entrusted their PII/PHI to Defendants. Plaintiff and the Class provided their PII/PHI to Defendants as part of Defendants' regular business practices.

136. Defendants should have been aware that they had a minimum duty to alert Plaintiff and Class members that their data was compromised "without unreasonable delay."

137. Thus, when Defendants took Plaintiff and Class members' PII/PHI, it entered into implied contracts with Plaintiff and Class members by which Defendants agreed to safeguard and protect such information and to keep such information secure and confidential. Implied in

these exchanges was a promise by Defendants to ensure that the PII/PHI of Plaintiff and Class members in its possession was secure.

138. Pursuant to these implied contracts, Plaintiff and Class members provided Defendants with their PII/PHI in order for Defendants to provide their services, for which Defendants are compensated. In exchange, Plaintiff understood, and Defendants agreed, among other things, that Defendants would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class members' PII/PHI; (3) protect Plaintiff and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) notify Plaintiff and Class members in compliance with state laws and regulations.

139. Implied in these exchanges was a promise by Defendants to take adequate measures to protect Plaintiff and Class members' PII/PHI, and notify Plaintiff and Class members where data safeguards failed.

140. A material term of this contract is a covenant by Defendants that they would take reasonable efforts to adequately secure that information. Defendants breached this covenant by allowing Plaintiff and Class members' PII/PHI to be accessed in the Data Breach.

141. Indeed, implicit in the agreement between Defendants and their customers was the obligation that both parties would maintain information securely and respond accordingly if that information was compromised.

142. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII/PHI in exchange for services by Defendants. These agreements were made by Plaintiff and Class members as Defendants' customers.

143. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class members would not have disclosed their PII/PHI to Defendants but for the prospect of utilizing Defendants' services. Conversely, Defendants presumably would not have obtained Plaintiff and Class members' PII/PHI if they did not intend to provide Plaintiff and Class members with their services.

144. Defendants were therefore required to reasonably safeguard and protect the PII/PHI of Plaintiff and Class members from unauthorized disclosure and/or use and, as promptly as reasonable, notify Plaintiff and Class members when it failed in that duty.

145. Plaintiff and Class members accepted Defendants' offer of services and fully performed their obligations under the implied contract with Defendants by providing their PII/PHI, directly or indirectly, to Defendants, among other obligations.

146. Plaintiff and Class members would not have entrusted their PII/PHI to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII/PHI.

147. Defendants breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff and Class members' PII/PHI.

148. Defendants' failure to implement adequate measures to protect the PII/PHI of Plaintiff and Class members violated the purpose of the agreement between the parties.

149. Defendants further failed to adequately and promptly notify Plaintiff and Class members that their PII had been compromised.

150. Instead of spending adequate financial resources to safeguard Plaintiff and Class members' PII/PHI, which Plaintiff and Class members were required to provide to Defendants,

Defendants instead used that money for other purposes, thereby breaching their implied contracts with Plaintiff and Class members.

151. As a proximate and direct result of Defendants' breaches of their implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered damages as described in detail above.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
On Behalf of the Nationwide Class Against All Defendants

152. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

153. Every contract has an implied covenant of good faith and fair dealing between the parties to it, which is an independent duty requiring every party in a contract to implement the agreement as intended, without using means to undercut the purpose of the transaction. This duty may be breached even when there is no breach of a contract's actual and/or express terms.

154. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

155. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII/PHI and failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members.

156. Defendants acted in bad faith in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them compensable injury in an amount to be determined at trial.

COUNT V
BREACH OF FIDUCIARY DUTY
On Behalf of the Nationwide Class Against All Defendants

157. Plaintiff realleges and reincorporates all previous paragraphs as if fully set forth below.

158. As a condition of obtaining services from Defendants, Plaintiff and Class Members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiff and Class Members. In light of this relationship, Defendants were and are required to act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiff and Class members' PII/PHI.

159. Defendants had and continue to have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the systems containing Plaintiff and Class members' PII/PHI, failing to comply with minimum data security practices, and otherwise failing to safeguard Plaintiff and Class members' PII/PHI that they collected.

160. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the

continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and/or (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT
On Behalf of the Nationwide Class Against All Defendants

161. Plaintiff incorporates the above allegations as if fully set forth herein.

162. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

163. Plaintiff conferred a benefit upon Defendants by using Defendants' services.

164. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff and Class members. Defendants also benefited from the receipt of Plaintiff and the Class members' PII/PHI as this was used by Defendants to administer services to Plaintiff and the Class.

165. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class members' services because Defendants failed to adequately protect their PII/PHI. Plaintiff and the proposed Class would not have provided their PII/PHI to Defendants or utilized their services had they known Defendants would not adequately protect their PII/PHI.

166. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VII
DECLARATORY JUDGMENT
On Behalf of the Nationwide Class Against All Defendants

167. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

168. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

169. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff and Class members' PII/PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII/PHI. Plaintiff alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury due to the compromise of her PII/PHI and remains at imminent risk that further compromises of her PII/PHI will occur in the future.

170. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure consumers' PII/PHI and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;

b. Defendants have breached their duty to Plaintiff and the Class by allowing the Data Breach to occur;

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII/PHI. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PII/PHI; and

d. Defendants' ongoing breaches of said duty continue to cause harm to Plaintiff and the Class.

171. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach with Defendants. The risk of another such breach is real, immediate, and substantial. If Defendants allow another data breach, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

172. Plaintiff and the Class, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' PII/PHI, and (2) to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class Members for their respective lifetimes; and

h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps they must take to protect themselves.

173. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with the law and industry standards to protect Plaintiff and Class members' PII/PHI.

174. The hardship to Plaintiff and Class members if an injunction were not issued exceeds the hardship to Defendants if an injunction were issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data

security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

175. Issuance of the requested injunction would not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiff and Class members whose PII/PHI would be further compromised.

COUNT VIII
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200
On Behalf of the California Subclass Against All Defendants

176. Plaintiff incorporates by reference and reallege each and every allegation above as though fully set forth herein.

177. Defendants and Plaintiff are "persons" as defined by the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17201.

178. The UCL states that "unfair competition shall mean and include any [1] unlawful, unfair or fraudulent business act or practice and [2] unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

179. By failing to take reasonable precautions to protect the PII/PHI of Plaintiff and the class members, Defendants have engaged in "unlawful," "unfair," and "fraudulent" business practices in violation of the UCL.

180. First, Defendants engaged in "unlawful" acts or practices because they violated multiple laws, including but not limited to the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures); the FTC Act, 15 U.S.C. § 45; and the common law, all as alleged herein.

181. Second, Defendants engaged in "unfair" acts or practices, including the following:

a. Defendants failed to implement and maintain reasonable data security measures to protect the Class members' PII/PHI. Defendants failed to identify foreseeable security risks, remediate identified risks, and adequately improve their data security in light of the highly sensitive nature of the data which it maintained and the known risk of cyber intrusions to companies storing sensitive medical and other personal information. Additionally, to the extent which Defendants may have identified a threat from duplicated account credentials, they did not implement timely reasonable security measures including mandatory MFA. Defendants' conduct, with little if any social utility, is unfair when weighed against the harm to the Class members whose PII/PHI has been compromised.

b. Defendants' failure to implement and maintain reasonable data security measures was also contrary to legislatively declared public policy that seeks to protect consumers' personal information and ensure that entities entrusted with PII/PHI adopt appropriate security measures. These policies are reflected in various laws, including but not limited to the FTC Act, 15 U.S.C. § 45; and the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures).

c. Defendants' failure to implement and maintain reasonable data security measures also led to substantial consumer injuries described herein, which are not outweighed by countervailing benefits to consumers or to competition.

182. Third, Defendants engaged in "fraudulent" acts or practices, including but not limited to the following:

a. Defendants omitted and concealed the fact that they did not employ reasonable safeguards to protect consumers' PII/PHI. Defendants knew or should have known that its data security practices were deficient. This is true because, among other things, Defendants were aware the extremely sensitive nature of the information they held, making this information particularly attractive to criminals, would make them a likely target of sophisticated cyberattacks. Defendants knew or should have known that their data security was insufficient to guard against those attacks.

b. Defendants also made express representations that their data security practices were sufficient to protect consumers' PII/PHI. Defendants knew the importance of this data and made express representations about their security In doing so, Defendants made implied or implicit representations that their data security practices were sufficient to protect consumers. Those representations were false and misleading.

183. Plaintiff and Class members transacted with Sutter in California by, among other things, providing their PII/PHI to Sutter and in using and maintaining their accounts and information in California. Plaintiff and Class members were deceived when they joined and used Sutter's services despite Defendants' deficient data security practices.

184. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class members were injured, lost money or property, and suffered the various types of damages alleged herein.

185. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendants' unfair competition including the loss of value of their breached PII/PHI.

186. Cal. Bus. & Prof. Code § 17203 states:

> Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments […] as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition.

187. Plaintiff and Class members are entitled to the injunctive relief requested herein to address Defendants' past and future acts of unfair competition.

188. Plaintiff and Class members are entitled to restitution of money and property that was acquired by Defendants by means of its unfair competition and restitutionary disgorgement of all profits accruing to Defendants as a result of its unfair business practices.

189. Plaintiff and Class members lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, as well as long term incalculable risk associated with medical fraud.

190. Further, if an injunction is not issued, Plaintiff and Class members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. It took Defendants over three month to disclose the cause and scope of the Breach, and adequate information is still not available. Plaintiff lacks an adequate remedy at law that will reasonably protect against the risk of such further breach.

191. Plaintiff and Class members seek all monetary and non-monetary relief allowed by the UCL, including reasonable attorneys' fees under Cal. Code of Civ. Procedure § 1021.5.

COUNT IX
VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.80, *et seq*.
On Behalf of the California Subclass Against All Defendants

192. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

193. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

194. The CCRA states: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access." Cal. Civ. Code § 1798.81.5(b).

195. The CCRA defines owns, licenses, and maintains as follows: "[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.'" Cal. Civ. Code § 1798.81.5(a)(2). 23andMe owns, licenses, and/or maintains the PII that was involved in the Data Breach.

196. The CCRA defines personal information, in pertinent part, as follows:

197. "Personal information" means either of the following: (A) An individual's first name or first initial and the individual's last name, in combination with any one or more of the

following data elements, when either the name or the data elements are not encrypted or redacted: …(iv) medical information. (v) health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (vii) genetic data.

198. Cal. Civ. Code § 1798.81.5(d)(1). The PII stolen in the Data Breach includes personal information that meets this definition.

199. Defendants failed to maintain reasonable data security procedures appropriate to the PII/PHI. Accordingly, Defendants violated Cal. Civ. Code § 1798.81.5(b).

200. Plaintiff and Subclass members were injured by Defendants' violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

201. Plaintiff and the Subclass members have suffered injuries including but not limited to actual damages, and in being denied a statutory benefit conferred on them by the California legislature.

COUNT X
VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code § 1750, *et seq*.
On Behalf of the California Class Against All Defendants

202. Plaintiff incorporates by reference and realleges each and every allegation above as though fully set forth herein.

203. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

204. Defendants are "persons" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

205. Plaintiff and Subclass members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

206. The acts and practices of Defendants were intended to and did result in the sales of products and services to Plaintiff and the Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

207. The representations and omissions of Defendants were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of patients' PII/PHI.

208. Had Defendants disclosed to Plaintiff and Subclass members that its data systems were not secure and, thus, vulnerable to attack, Plaintiff and Subclass members would not have purchased their services or would have paid less to account for its inadequate data security. Defendants were trusted with sensitive and valuable PII/PHI regarding millions of consumers, including Plaintiff. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

209. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII/PHI; overpayment for Defendants' services; loss of the value of access to their PII/PHI; the value of identity protection services made necessary by the Breach, the increased risk of targeted attacks based on ethnicity, and the long term risks and costs associated with loss of sensitive medical data.

210. Plaintiff, on behalf of herself all class members, demands judgment against Defendant under the CLRA for injunctive relief.

211. Pursuant to Cal. Civ. Code § 1782(a), Plaintiff will serve Defendants with notice of their alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Defendants fail to provide appropriate relief for their violations of the CLRA, Plaintiff will amend this Complaint to seek monetary damages.

212. Notwithstanding any other statements in this Complaint, Plaintiff does not seek monetary damages in conjunction with her CLRA claim—and will not do so—until this thirty-day period has passed.

COUNT XI
VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
Cal. Civil Code Section 56.06
On Behalf of the California Subclass Against All Defendants

213. Defendants are providers of healthcare under Cal. Civ. Code § 56.06, subdivisions (a) and (b), because they maintain medical information and offer software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or make the information available to a health care provider, or for the diagnosis, treatment, or management of a medical condition.

214. Defendants are therefore subject to the requirements of the CMIA and obligated under Section 56.06 subdivision (e) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information that it maintains on behalf of users.

215. The CMIA defines medical information as meaning any "individually identifiable information" in possession of or derived from "a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." The information Defendants maintained and disclosed is medical information because it relates to medical history, and was individually identifiable because it included information, including name and location, which "alone or in combination with other publicly available information reveals the identity of the individual."

216. Defendants violated Cal. Civ. Code Section 53.06(e) because they did not maintain the confidentiality of Plaintiff and Subclass members' medical information. This

identifiable information was shared with third parties including criminal third parties and hackers, which are now selling the information on the dark web. This disclosure was not authorized by the individual.

217. This negligent disclosure is in violation of Cal. Civ. Code Section 53.06(e) Accordingly, Plaintiff and Subclass members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to Cal. Civ. Code Section 56.36(c); and reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seek judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and Subclass and their counsel as Class Counsel;

(b) For an order declaring the Defendants' conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class and Subclass on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief;

(h) For declaratory and/or injunctive relief, as set forth herein; and

(i) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: January 10, 2024

/s/ Amber L. Schubert

Robert C. Schubert
Amber L. Schubert
Schubert Jonckheer & Kolbe LLP
2001 Union Street, Suite 200
San Francisco, California 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Counsel for Plaintiff and the Putative Class

Exhibit 1

Welltok®

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 31, 2023

K2585-L01-0028601 T00091 P003 ********SCH 5-DIGIT 94133
MOIRA DUFFY
APT 16
350 FRANCISCO ST
SAN FRANCISCO, CA 94133-1916

Notice of Data Breach

Dear Moira Duffy:

Welltok, Inc., writes on behalf of Sutter Health to inform you of an event that may affect the security of your personal information. Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Sutter Health and received your information in connection with these services. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook an exhaustive and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

What Information Was Involved? While we have no evidence that any of your information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following types of your information may have impacted: your name and date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 800-628-2141, which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and on Saturday and Sunday between the hours of 8:00 a.m. to 5:00 p.m. Pacific Time excluding major U.S. holidays.

We apologize for any inconvenience to you and remain dedicated to protecting the information in our care.

Sincerely,

Welltok, Inc.

K2585-L01

B107736

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** Febraury 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **VTCR5BBKT**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 800-628-2141 by Febraury 29, 2024. Be prepared to provide engagement number B107736 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 21 Rhode Island residents impacted by this event.

0028601

K2585-L01

B107736